(12) **EUROPEAN PATENT APPLICATION**

(84) Designated Contracting States: **AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE** Designated Extension States: **AL LT LV MK RO SI**	(72) Inventor: **Wajs, Andrew Augustine** **2023 AA Haarlem (NL)**
(71) Applicant: **Irdeto Access B.V.** **2132 HD Hoofddorp (NL)**	(74) Representative: **de Vries, Johannes Hendrik Fokke** **De Vries & Metman** **Overschiestraat 180** **1062 XK Amsterdam (NL)**

(54) **Method for controlling the use of a program signal in a broadcast system, and control device for a receiver for carrying out such a method**

(57) In a method for controlling the use of a program signal in a broadcast system, comprising one or more broadcasters and a number of receivers, at least a part of the receivers can be provided with a storage medium for storing program signals. The program signal comprises content signals of a first and a second type, wherein the second type of content signals is inserted in time slots in the first type of content signals. At least the first type of content signals is scrambled using control words as scrambling keys to obtain a scrambled program signal. The program signal is scrambled using control words as scrambling keys and the scrambled program signal is broadcasted together with entitlement control messages (ECM's) containing the control words in an encrypted manner using a second key. Decrypting means are provided at each receiver for retrieving the control words from the ECM's by decrypting the ECM's, wherein the control words are delivered by the decrypting means for descrambling the program signal. At least a plurality of ECM's comprises control information to control the decrypting means in such a manner that at least the time slots for second type of content signals are maintained in the first type of content signals.
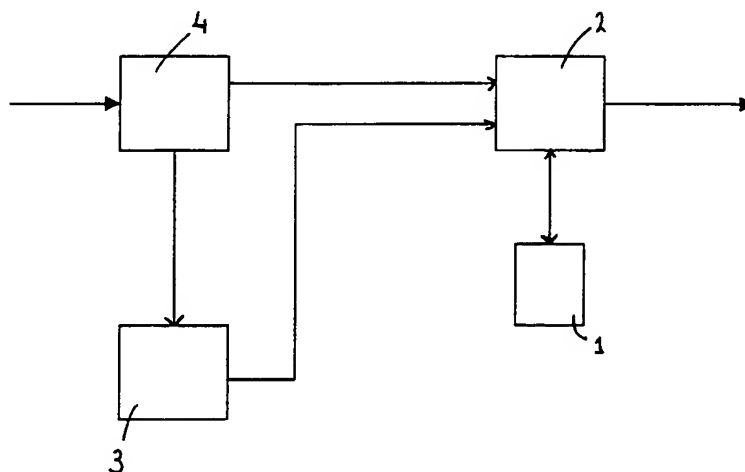
Fig. 1

Description

[0001]   The invention relates to a method for control-. ling the use of a program signal in a broadcast system, comprising one or more broadcasters and a number of receivers, at least a part of the receivers preferably having a storage medium for storing program signals, wherein the program signal comprises content signals of a first and a second type, wherein at least the first type of content signals is scrambled using control words as scrambling keys to obtain a scrambled program signal and wherein the scrambled program signal is broadcasted together with entitlement control messages (ECM's) containing the control words in an encrypted manner using a second key, wherein decrypting means are provided at each receiver for retrieving the control words from the ECM's by decrypting the ECM's, and wherein the control words are delivered by the decrypting means for descrambling the program signal. The invention further relates to a control device for a receiver for carrying out such a method, comprising decrypting means for retrieving the control words from ECM's by decrypting the ECM's, and for delivering decrypted control words for descrambling a program signal.

[0002]   Recently audio/video devices has become available, wherein the device is provided with a storage medium having sufficient storage capacity to store hours of audio/video programs. With such audio/video devices it is possible to use a remote editing agent in the receiver to construct a broadcasting station within the device. The remote editing agent causes video and/ or audio clips to be presented to the viewer in a continuous sequence simulating a broadcast service. The sequence can be determined by direct user interaction, user settings or intelligent analysis within the receiver of the user's behaviour.

[0003]   In many cases, a program signal includes both content signals (or more generally content signals of a first type) and advertisement signals (or more generally content signals of a second type), wherein selling advertisement time slots in the complete program is an important income source of the broadcaster. With the availability of audio/video devices of the above-mentioned type, the remote editing agent can use the user interaction/profile to select which advertisements should be inserted in the advertisement slots in the program signal. In this manner a broadcaster can resell the same advertisement slots to many advertisers and the advertisements can be better targeted to the viewers. This way of tuning advertisement slots to the viewer requires to add data to the program signal with flags indicating the insertion points to insert advertisements in the advertisement slots and data describing the type of advertisements and programs, respectively. However a program signal with flags to indicate the advertisement slots is open to use by unauthorized third parties which can reprogram the receivers to use the program signal provided by the broadcaster to insert their own adver-

tisements or to remove the advertisement slots completely.

[0004]   The invention aims to provide a method of the above-mentioned type, wherein unauthorized use of a program signal is prevented in an efficient manner.

[0005]   According to the method of the invention at least a plurality of ECM's comprises control information to control the decrypting means in such a manner that at least the time slots for second type of content signals are maintained in the first type of content signals.

[0006]   In this manner a method is obtained, wherein unauthorised use of the program signal is prevented, because the decrypted ECM's provided by the broadcaster provide control on the use of the signal, in particular on maintaining the time slots in the first type of content signal.

[0007]   Preferably, the ECM's comprise first ECM's for the first type of content signals and second ECM's for the second type of content signals, wherein at least a plurality of first and second ECM's is provided with control information, wherein the decrypting means checks the control information and delivers decrypted control words of the first or second ECM's in accordance with the control information to descramble content signals of the first or second type, respectively.

[0008]   The invention further provides a control device of the above-mentioned type characterized in that the decrypting means is adapted to check the control information of the decrypted ECM's and to insert a time slot in the first type of content signals as indicated by the control information.

[0009]   The invention will be further explained by reference to the drawings, in which an embodiment of the method and control device of the invention are shown by way of example.

[0010]   Fig. 1 shows in a very schematic manner an embodiment of a control device of the invention.

[0011]   Fig. 2 shows a flow diagram to explain an embodiment of the method of the invention.

[0012]   Fig. 3 shows a flow diagram to explain a second embodiment of the method of the invention.

[0013]   It is noted that in the following examples the insertion of advertisements into a content signal, such as a show or a film, is described. However the invention generally relates to a method for controlling the use of a program signal, wherein the program signal comprises a first type of content signals, i.e. the show or film or the like, and a second type of content signals, for example advertisement signals, wherein the second type of content signals can be inserted into the first type of content signals under the control of the broadcaster.

[0014]   In the method described the program signal that is broadcasted is scrambled irrespective whether it is a pay service or a service based upon advertisement as source of income. The scrambling is carried out in a usual manner according to a conditional access system with a key hierarchy. It is noted that the structure of the conditional access system and the descrambling/en-

cryption techniques used are not part of the present invention. According to the invention, the conditional access system is used to manage the insertion of the advertisements into the program signal.

[0015] The control device shown in fig. 1 is adapted to operate according to a conditional access system, wherein so-called entitlement control messages or ECM's are broadcasted together with the program signal, wherein the ECM's comprise the control words or first keys which are used to scramble the clear program signal. The control words are encrypted using a second key which is available in the control device, in case of the embodiment shown in fig. 1 in a smart card 1. The smart card 1 decrypts the ECM's to provide the clear control words to a unit 2 for descrambling the scrambled content signal. The output of the unit 2 provides the clear audio/video signals. The input to the descrambling unit 2 may be a compressed signal, in which case the unit 2 also operates to decompress the signal. The input signals can be retrieved from a storage medium 3, for example a hard disk with large capacity, or directly from a demodulator/demultiplexer 4. The signals stored on the storage medium 3 may come from the demodulator/demultiplexer 4. This part of the control device is not part of the present invention and will therefore not be described further.

[0016] Both the content program signal and the advertisement signal have their corresponding ECM's inserted, i.e. content or first ECM's and advert or second ECM's, respectively. Although in this embodiment the advertisement signal is scrambled with advert ECM's, the advertisement signal may be sent in the clear or scrambled using the control word of the last content ECM. This means that it is also possible to use only one type of ECM's.

[0017] As the program signal is played back the appropriate ECM's are sent to the smart card and these ECM's are used to control the use of the complete program signal. To this end, the content ECM's may carry control information including a content sequence identifier. This control information can include information on the content and rules for insertion of the advertisement signals into the content. These rules may for example indicate specific advertisements which should be inserted into the specific content signal, for example in case the broadcaster has sold advertisement slots in specific films, shows or the like. It will be clear to the skilled person that the storage medium 3 will have stored several types of advertisement signals, so that different control devices according to fig. 1 can insert different advertisements depending on user settings or analysis of user behaviour. A further possibility as a rule for insertion of different advertisements is insertion in dependence of the time of the day.

[0018] The ECM's of the advertisement signals also may carry control information including a sequence identifier. The control information may include information identifying the advertising material, information

specifying how many advert ECM's there are in the sequence of ECM's that delivers control words for one advertisement and the order of ECM's. Typically, a conditional access system changes the control word every few seconds so that with an advertising slot of for example 30 seconds, there may be several ECM's per advertising slot.

[0019] The control information may further include timing information specifying a delay between ECM's. In this manner fast forwarding of the advertisements or submission of advert ECM's without actually processing the content can be prevented. The smart card 1 is provided with a real time clock and checks the delay specified by the ECM and if this delay has not passed, the smart card 1 does not accept the next or any other ECM in the sequence before the delay has actually passed. In this manner the advertising slot is enforced during the playback of the program signal.

[0020] It is noted that at least a part of the content ECM's may also include timing information in the control information, in particular in ECM's just before and after an advertisement slot to prevent a start of fast forwarding just before the advertisement slot. The sequence identifiers in both types of ECM's are used to signal the smart card 1 a jump to a new point in the program signal.

[0021] According to the method of the invention described various rules for insertion of advertisements can be used.

[0022] In an embodiment wherein only one type of ECM's are used, the decryption of an ECM can be made dependent on the decryption of a previous ECM. For example by using the sequence identifier of the ECM's a next ECM is only used to obtain the control word if the previous ECM has indeed been used. Skipping a part of the program, in particular the time slot for advertisements is prevented in this manner. As an alternative the same result can be obtained by providing timing indices within one type of ECM's. The timing information in the ECM's will enforce a break in the normal program for insertion of the adverts.

[0023] Fig. 2 shows an embodiment wherein timing is used to insert the advertisements into the content program signal. By way of example a slot of one minute of advertisement could be inserted into each five minutes of program content. To this end the control information of the content ECM's carry information to count down until the advertisement insertion slot. In the flow diagram shown in fig. 2, each ECM extracted from the program signal is checked by the smart card on timing information and if the time delay is correct, the ECM is checked on whether or not it is an advert ECM. If it is a content ECM, the content ECM counter is incremented. Depending on the count of the counter, a flag is set to indicate that an advert ECM should be extracted in the next cycles. After outputting the control word to the descrambler 2, a next ECM is extracted. If an advert ECM is detected by the smart card, a counter for advert ECM's is incremented and the output control word is provided

to the descrambler 2. When the advertisement slots have passed, the ECM flag is reset to content and a next content ECM is extracted. If the advertisement slot has not yet passed, a next advert ECM is extracted.

[0024] As an alternative to the operation shown in the flow diagram of fig. 2, only the last ECM before the advertisement insertion point could have an indication to instruct the smart card to start an advertisement slot.

[0025] During processing advert ECM's, the smart card 1 ensures by checking the time delay that the delay between ECM's is such that the specified advertisement duration is maintained even if the user tries to fast forward during the advertisement slot.

[0026] As mentioned above, in this example, the content ECM's could contain control information which indicates that only specific advertisements should be inserted into the next advertisement slot. The smart card will then only allow corresponding advert ECM's to be processed.

[0027] It is possible that the user of the control device switches to another channel during the advertisement slot. In order to guarantee that the advertisement is viewed, the smart card 1 can maintain a log of the program that has been watched by retrieving the program signal from the storage medium 3. When the user returns to that channel, the smart card enforces that the correct advertisement sequence is watched before the next part of program content becomes available.

[0028] In fig. 3 a flow diagram of a second embodiment is shown, wherein for both the content ECM's and the advert ECM's a counter is used, wherein the control information of the content ECM's indicates a threshold for the amount of viewing of the program content which must occur before an advertisement can be inserted. Once the threshold, i.e. a minimum amount of viewing time, has been reached the smart card 1 may be programmed such that it waits for an appropriate insertion point or immediately stops processing content ECM's until a predetermined number of advert ECM's are processed.

[0029] In this embodiment the control information of the content ECM's may also indicate the appropriate insertion point for the advertisement slot. In this manner the advertisements are not randomly inserted in the middle of a scene but only at a scene boundary for example. Of course, the control information of the content ECM's may also indicate a maximum value of program viewing time and if exceeded, the smart card 1 does not wait until an appropriate insertion point but immediately starts to process advert ECM's.

[0030] A program signal may include one or more ECM's having a decision rule as part of the control information, which decision rule provides the user the possibility to select a viewing mode with a particular entitlement to watch the content without advertisement insertion. This particular entitlement may be subscription, pay per view or the like.

[0031] As an alternative it can be guaranteed that an advertisement slot is not deleted or skipped by providing control information in the last ECM or plurality of ECM's before the advertisement slot indicating the rate at which ECM's are allowed to be processed or the delay before the next ECM is allowed to be processed. For example, this control information instructs the control device to wait for two minutes before the next ECM can be processed.

[0032] Although in the above embodiments the invention is explained when using stored content, the invention can be used in the same manner in watching or listening normal broadcast signals. The advert ECM's can be used to check whether the user has not surfed to another channel. If the user did surf to another channel access to the content of the channel using the described control method, can then be denied for a predetermined period for example.

[0033] In the above-described embodiments, a control device is used having a hardware smart card for processing the ECM's as in a conventional conditional access system. According to an embodiment of the invention described, the function of the smart card regarding processing of ECM's can be carried out by a software module which is executed in a microprocessor of the descrambler 2. This software module is provided by the broadcaster and is downloaded over the air into the descrambler 2 and can be changed regularly to prevent unauthorised persons to reprogram the descrambler 2, for example to completely delete the advertisement slots or to insert there own advertisements.

[0034] The invention is not restricted to the above described embodiment and can be varied in a number of ways within the scope of the following claims.

Claims

1. Method for controlling the use of a program signal in a broadcast system, comprising one or more broadcasters and a number of receivers, at least a part of the receivers preferably having a storage medium for storing program signals, wherein the program signal comprises content signals of a first and a second type, wherein the second type of content signals is inserted in time slots in the first type of content signals, wherein at least the first type of content signals is scrambled using control words as scrambling keys to obtain a scrambled program signal and wherein the scrambled program signal is broadcasted together with entitlement control messages (ECM's) containing the control words in an encrypted manner using a second key, wherein decrypting means are provided at each receiver for retrieving the control words from the ECM's by decrypting the ECM's, and wherein the control words are delivered by the decrypting means for descrambling the program signal, characterized in that at least a plurality of ECM's comprises control infor-

mation to control the decrypting means in such a manner that at least the time slots for second type of content signals are maintained in the first type of content signals.

2. Method according to claim 1, wherein a real time clock is operated at the receiver side, wherein the control information of an ECM near the beginning of a time slot for the second type of content signals indicates a delay before a next ECM can be decrypted by the decrypting means.

3. Method according to claim 1, wherein the ECM's comprise first ECM's for the first type of content signals and second ECM's for the second type of content signals, wherein at least a plurality of first and second ECM's is provided with control information, wherein the decrypting means checks the control information and delivers decrypted control words of the first or second ECM's in accordance with the control information to descramble content signals of the first or second type, respectively.

4. Method according to claim 3, wherein the control information of said plurality of ECM's comprises timing information, wherein a real time clock is operated at the receiver side, wherein the decrypting means checks the timing information of each ECM by means of the real time clock and continues to deliver control words of the ECM's for descrambling the program signal only if the timing information corresponds with the time indication provided by the real time clock.

5. Method according to claim 4, wherein a sequence identifier and a minimum delay which should pass before a next ECM should be decrypted are added to said plurality of ECM's as timing information, wherein the decrypting means checks the time passed by means of the real time clock and continues to deliver a next control word only if the time passed corresponds with the minimum delay.

6. Method according to any one of claims 1-5, wherein the control information of the ECM's comprises a sequence identifier including an index number of the previous and/or next ECM's, wherein the decrypting means checks the index number of a received ECM against the expected index number, wherein the control word is only provided if the index number received matches the expected index number.

7. Method according to claim 1, wherein the control information of an ECM comprises information on the insertion of the second type of content signals in the first type of content signals.

8. Method according to claim 3 and 7, wherein at least a plurality of first ECM's provides control information for the decrypting means indicating the decrypting means to use a plurality of second ECM's, wherein the control information may comprise timing information on the time period for using first ECM's and on the time period for using second ECM's, and information on the point within the first type of content signals for inserting the second type of content signals.

9. Method according to claim 8, wherein the second type of content signals comprise content signals with corresponding ECM's representing various contents, wherein the control information of at least a part of said plurality of first ECM's comprises selection identifiers for allowing only a selected content signal with corresponding ECM's to be used for insertion into the first type of content signals as second type of content signals, wherein in particular the selection identifiers select the content signal depending on the time of the day.

10. Method according to claim 8 or 9, wherein the decrypting means enforces the receiver to use all second ECM's corresponding to the time period indicated for using the second ECM's independent of the receiver being tuned to the corresponding program signal source.

11. Method according to any one of the preceding claims, wherein the ECM's are inserted in the program signal in synchronisation with the change of the control words used to scramble the program signal.

12. Method according to any one of the preceding claims, wherein the decrypting means is provided as a software module broadcasted by a broadcaster, wherein the software module is executed in the receivers, wherein the software module is regularly changed by the broadcaster.

13. Method according to claim 3, wherein an ECM of the first ECM's for the first type of content signals comprises control information to switch the decrypting means to deliver only first ECM's for the first type of content signals if the decrypting means indicate a viewing mode allowing the use of the first content signals only.

14. Control device for a receiver for carrying out the method according to any one of the preceding claims, comprising decrypting means for retrieving the control words from ECM's by decrypting the ECM's, and for delivering decrypted control words descrambling a program signal, characterized in that the decrypting means is adapted to check the

control information of the decrypted ECM's and to insert a time slot in the first type of content signals as indicated by the control information.

15. Control device according to claim 14, wherein the decrypting means delivers decrypted control words of the first or second ECM's in accordance with the control information to descramble content signals of the first or second type, respectively.

16. Control device according to claim 14 or 15, further comprising a real time clock, wherein the decrypting means is adapted to check the timing information in the control information of each ECM by means of the real time clock and to continue to deliver control words of the ECM's for descrambling the program signal only if the timing information corresponds with the time indication provided by the real time clock.
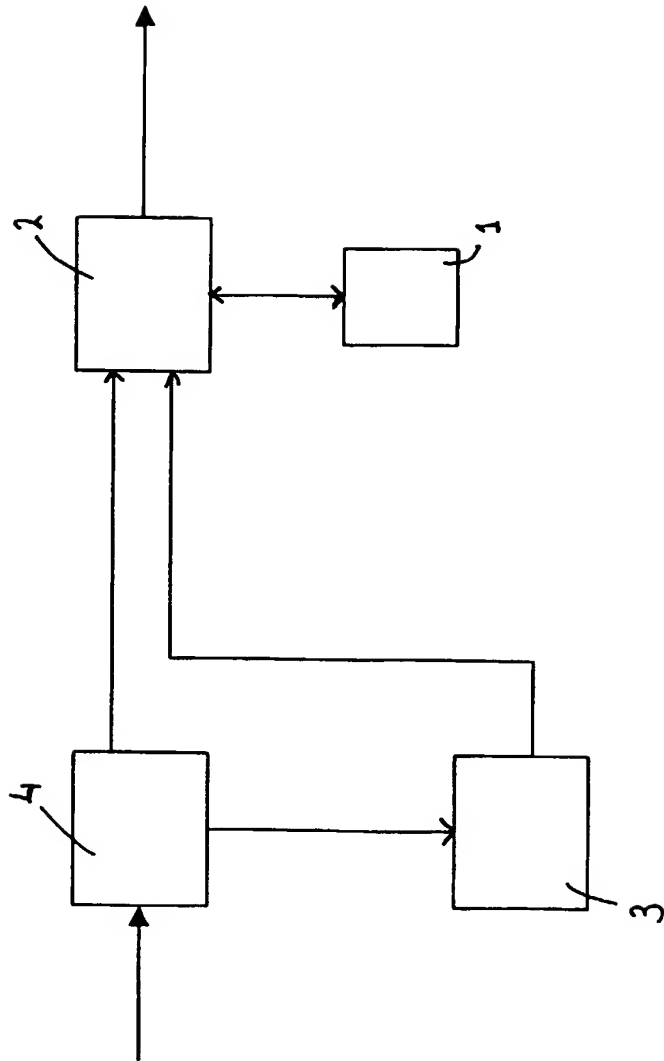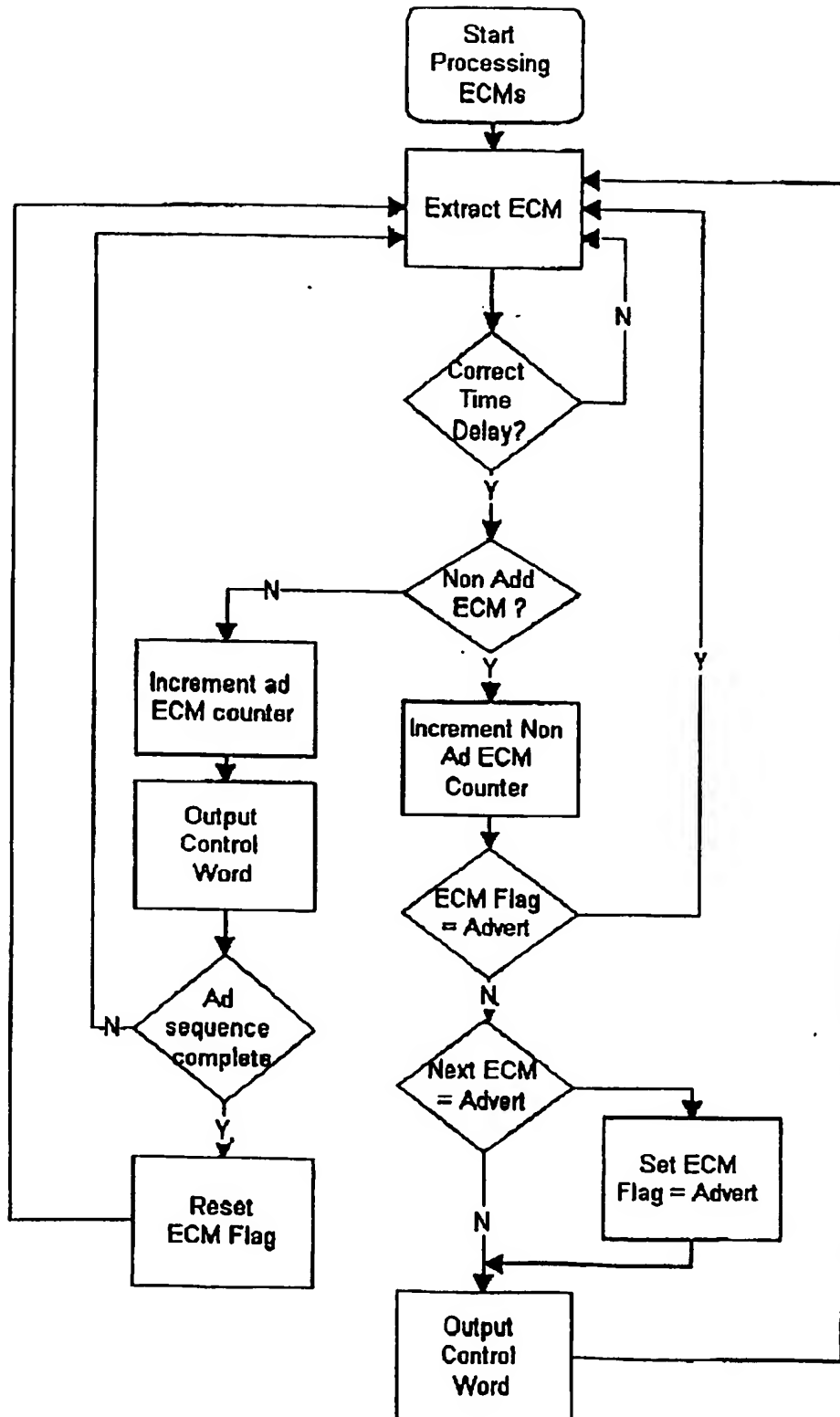
5

10

15

20

25

30

35

40

45

50

55

Fig. 1

```
                           ┌──────────────┐
                           │    Start     │
                           │  Processing  │
                           │     ECMs     │
                           └──────┬───────┘
                                  │
                                  ▼
        ┌──────────────────► ┌──────────────┐ ◄──────────────────┐
        │       ┌──────────► │  Extract ECM │ ◄──────────────┐    │
        │       │            └──────┬───────┘ ◄─────────┐    │    │
        │       │                   │        ──┐        │    │    │
        │       │                   ▼          │ N      │    │    │
        │       │              ╱ Correct ╲ ────┘        │    │    │
        │       │             ╱   Time    ╲             │    │    │
        │       │             ╲  Delay?   ╱             │    │    │
        │       │              ╲    │    ╱              │    │    │
        │       │                   │ Y                 │    │    │
        │       │                   ▼                   │    │    │
        │       │    N         ╱  Non Add ╲             │    │    │
        │       │   ◄─────────╱    ECM ?   ╲            │ Y  │    │
        │       │   │          ╲           ╱            │    │    │
        │       │   ▼           ╲    │    ╱             │    │    │
        │  ┌──────────┐              │ Y                │    │    │
        │  │Increment ad│            ▼                  │    │    │
        │  │ECM counter │    ┌──────────────┐           │    │    │
        │  └─────┬────┘      │Increment Non │           │    │    │
        │        │          │  Ad ECM       │           │    │    │
        │        ▼          │  Counter      │           │    │    │
        │  ┌──────────┐      └──────┬───────┘           │    │    │
        │  │  Output  │             │                   │    │    │
        │  │ Control  │             ▼                   │    │    │
        │  │   Word   │        ╱ ECM Flag ╲ ────────────┘    │    │
        │  └─────┬────┘        ╲ = Advert  ╱                 │    │
        │        │              ╲   │    ╱                   │    │
        │        ▼                  │ N                      │    │
        │  N  ╱  Ad   ╲             ▼                         │    │
        │ ◄──╱sequence ╲       ╱ Next ECM ╲ ──────►          │    │
        │    ╲complete ╱       ╲ = Advert  ╱        │         │    │
        │     ╲   │   ╱         ╲   │    ╱          ▼         │    │
        │         │ Y               │ N        ┌──────────┐   │    │
        │         ▼                 │          │ Set ECM  │   │    │
        │  ┌──────────┐             │          │Flag = Advert │   │
        │  │  Reset   │             ▼          └─────┬────┘   │    │
        └──│ ECM Flag │        ┌──────────┐          │        │    │
           └──────────┘        │  Output  │ ◄────────┘        │    │
                               │ Control  │───────────────────┘    │
                               │   Word   │────────────────────────┘
                               └──────────┘
```

fig. 2

Start
Processing
ECMs

Extract ECM

Correct
Time
Delay?

N

Non Add
ECM ?

N

Y

Increment ad
ECM counter

Increment Non
Ad ECM
Counter

Output
Control
Word

ECM
Counter>
Max?

Y

Ad
sequence
complete

N

Output
Control
Word

Y

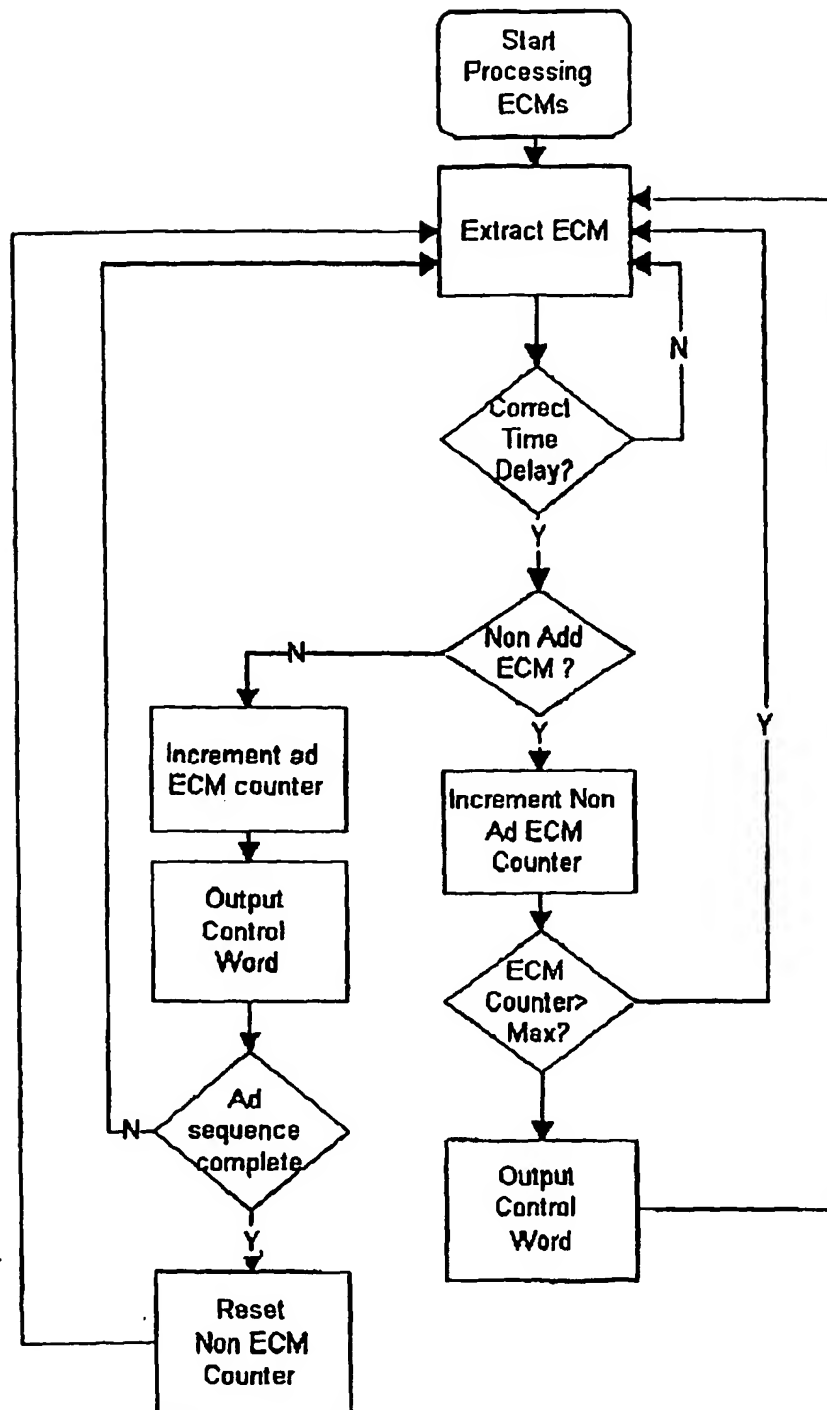Reset
Non ECM
Counter

fig.3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 99 20 4482

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 815 671 A (MORRISON ERIC FRASER) 29 September 1998 (1998-09-29) * column 2, line 46 – column 4, line 13 * * column 5, line 1 – column 10, line 54; figures 2-6 *	1,3,4, 7-9, 13-16	H04N7/167 H04N7/16
Y	EP 0 912 052 A (CANAL PLUS SA) 28 April 1999 (1999-04-28) * column 5, line 55 – column 7, line 36 * * column 9, line 20-57; figures 2-4 *	1,3,4, 7-9, 13-16	
A	EP 0 926 892 A (INFORMATION BROADCASTING LAB I ;MATSUSHITA ELECTRIC IND CO LTD (JP) 30 June 1999 (1999-06-30) * column 4, line 42 – column 5, line 5 * * column 7, line 55 – column 13, line 3; figures 1,9-20 *	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 July 2000	Pantelakis, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**   EP 99 20 4482

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-07-2000

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5815671	A	29-09-1998	NONE		
EP 0912052	A	28-04-1999	AU	9092698 A	12-04-1999
			EP	1018265 A	12-07-2000
			WO	9916244 A	01-04-1999
			NO	20001529 A	25-05-2000
			ZA	9808703 A	01-04-1999
EP 0926892	A	30-06-1999	JP	11196360 A	21-07-1999
			JP	11196361 A	21-07-1999
			CN	1235476 A	17-11-1999